



Будьте **УВАЖНІ** до будь-яких листів, яких не очікували.



Помітили **ПІДОЗРІЛУ** діяльність? Повідомте ІТ-спеціалісту вашої організації або CERT-UA.



Завжди робіть **РЕЗЕРВНУ** копію даних.



Регулярно змінюйте **ЛОГІНИ ТА ПАРОЛІ АДМІНІСТРАТОРА НА РОУТЕРАХ WiFi ТА КАМЕРАХ.**



Обмежте введення свого **НОМЕРА ТЕЛЕФОНУ**, що прив'язаний до онлайн-банкінгу, в будь-які онлайн-форми.



РЕГУЛЯРНО ОНОВЛЮЙТЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ.



Залишайте якомога **МЕНШЕ** персональних даних в інтернеті.

КОРИСНІ ОСВІТНІ МАТЕРІАЛИ ТА СЕРІАЛИ, ЯКІ ДОПОМОЖУТЬ ГЛИБШЕ РОЗІБРАТИСЯ В ТЕМІ:

Дія.Цифрова освіта — це національний онлайн-портал із розвитку цифрової грамотності, на якому можна безоплатно навчатися в захопливому форматі освітніх серіалів. Понад 800 000 громадян вже зареєструвалися та почали навчання на порталі.

Освітній серіал «Основи кібергігієни» на порталі Дія.Цифрова освіта



Це 9 серій тривалістю 4-7 хвилин, які дозволять:

- розуміти суть соціальної інженерії та психології впливу;
- безпечно користуватися браузером та загальною мережами WiFi;
- розмежовувати використання особистої та службової поштових скриньок;
- ознайомитися з роллю фізичної безпеки в кіберзахисті організації;
- розібратися у видах маніпуляцій з інформацією у кіберсфері.

Експрес-тест на цифрову грамотність, який за кілька коротких запитань допоможе вам визначити рівень цифрових навичок та дізнатися нові факти про безпеку онлайн.



Освітній серіал «Кіберняні» на порталі Дія.Цифрова освіта

З цього курсу ви дізнаєтесь, як мінімізувати ризики втрати вашої приватної, чутливої інформації, як попередити кібератаку або кібершахрайство, та як швидко відновитися після них у разі, якщо вони все ж таки сталися.



Міністерство
цифрової трансформації
України



Організація з безпеки та
співробітництва в Європі
Координатор проектів в Україні

Дія

Цифрова
освіта



МІЖНАРОДНА ФУНДАЦІЯ
ВИБОРЧИХ СИСТЕМ



1. СТАТИСТИКА КІБЕРАТАК У 2020 РОЦІ

2020 року фахівці CYBER POLYGON з безпеки нарахували понад **900 кіберзлочинців** і понад **1 млрд шкідливих програм**. Загрози класифіковані за трьома рівнями: **Нижній рівень (94%)** — найпримітивніші атаки.

- **фішингові сайти на тему COVID-19: допомога в отриманні допомог та компенсацій, підроблені сертифікати про вакцинації та QR-коди;**
- **шахрайства з доставкою товарів і послуг;**
- **дзвінки шахраїв, які представляються службою безпеки банку і вимагають дані карток.**

Середній рівень (5%) — це атаки програм-вимагачів, кожна четверта з яких припала на корпоративних користувачів. Яскраві приклади:

- **атака на мережу американських заправок Colonial Pipeline: привела до їх повного колапсу;**
- **атака на ірландську службу охорони здоров'я: в результаті люди не могли записатися на вакцинацію або на прийом до лікаря.**

Верхній рівень (близько 1%) — найскладніші та точно спрямовані атаки, на розслідування яких іноді витрачаються роки.



Будьте уважні до будь-яких листів, яких не очікували.

2. Грудень 2018: кібератака проти німецьких політиків



Хакери оприлюднили **особисті дані** сотень німецьких політиків, журналістів і знаменитостей. Цю атаку назвали одним із найбільших **порушень кібербезпеки** країни.

Витік інформації містив:

- мобільні **номери** та **адреси** депутатів;
- **електронні листи**;
- **дані** інтернет-переписки та кредитних карток;
- копії **документів**, що посвідчують особу, та договори оренди;
- **голосові повідомлення** від партнерів та дітей.

Дані було зламано з приватних облікових записів електронної пошти, а також їхніх записів у соціальних медіа, як-от Facebook та Twitter.

Принаймні два депутати помітили збої в роботі своїх облікових записів за декілька місяців до атаки.

Помітили підозрілу діяльність? Повідомте ІТ-спеціалісту вашої організації або CERT-UA.

3. Як вірус «Ретуга» видалив інформацію

Ретуга і його пізні версії вражали комп'ютери через операційну систему (ОС) Microsoft Windows. Вони зашифровували файли і дані для завантаження ОС. Потім вірус вимагав викуп у біткоїнах, але коди для розшифровки не допомагали. Вони, навпаки, знищували всі дані на жорсткому диску. При цьому вірус отримував повний контроль над усією інфраструктурою компанії.

Вірус торкнувся компаній і держорганів Європи, США, Австралії, Росії, України, Індії, Китаю.

В Україні постраждало понад **300 компаній**:

- «Запоріжжяобленерго»;
- «Дніпроенерго»;
- Київський метрополітен;
- українські мобільні оператори «Київстар», LifeCell і «Укртелеком»;
- корпорація «Ашан»;
- ПриватБанк;
- аеропорт Бориспіль.

10% пам'яті всіх комп'ютерів в країні виявилось стертою.

Загальна сума збитку від діяльності хакерів становить більше **\$10 млрд.**



10% пам'яті всіх комп'ютерів в країні виявилось стертою



\$10 млрд становить загальна сума збитку від діяльності хакерів

В Україні постраждало понад 300 компаній



«Запоріжжя-обленерго»



Київський метрополітен



«Дніпроенерго»



ПриватБанк



корпорація «Ашан»



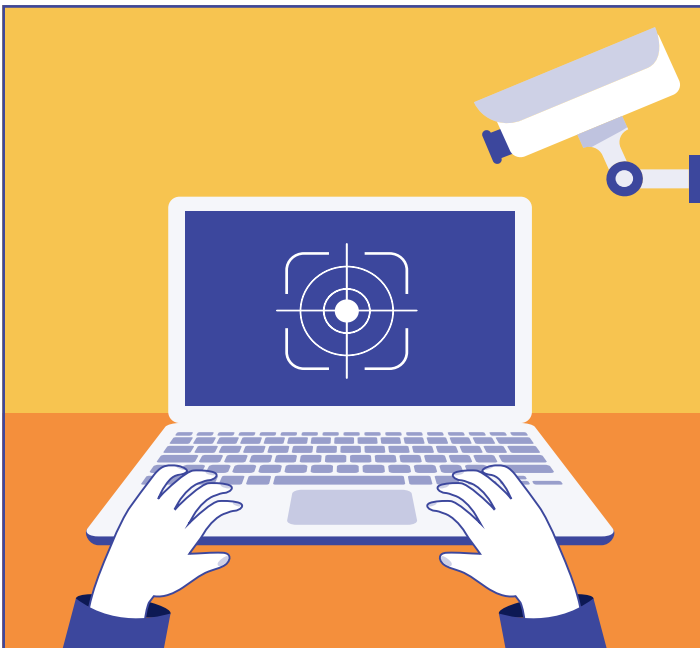
аеропорт Бориспіль



українські мобільні оператори «Київстар», «LifeCell» і «Укртелеком»

Завжди робіть резервну копію даних.

4. Як можуть атакувати ваші камери та WiFi?



Недавній **Linux-троян** для Raspberry Pi **знаходить** пристрої з логіном і паролем, які власники не змінили після покупки, змінює пароль, а потім **встановлює** додаток для майнінгу криптовалюти. Ідея та реалізація гранично прості.

Існують пошукові системи Інтернету речей, в яких можна знайти величезну кількість вразливих **IP-камер**, що мають стандартні дані для входу адміністратора.

Скористатися ними може практично будь-хто. Ці камери розташовані в магазинах, на заводах, складах, автостоянках.

Більш того, вони є і в будинках, гаражах, спальнях та вітальнях.

Люди, які використовують такі **«загальнодоступні» камери**, і не підозрюють, що сторонні можуть **спостерігати** за кожним їхнім кроком.

Регулярно змінюйте логіни та паролі адміністратора на роутерах WiFi та камерах.

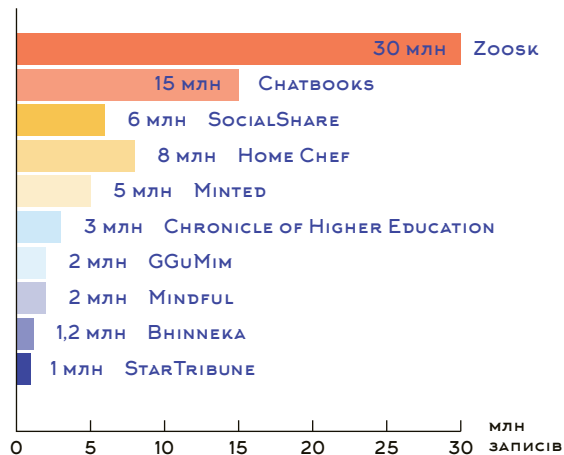
5. ХАКЕРИ ВИКЛАЛИ В ДАРКНЕТ ОСОБИСТІ ДАНІ 73 МІЛЬЙОНІВ ЛЮДЕЙ

Хакерське угруповання **SHINYHUNTERS** зламало бази даних і отримало доступ до особистої інформації **73 мільйонів осіб** у травні 2020 року. Серед викрадених баз даних, що вже продаються в даркнеті, такі відомі **10 компаній**:

- Сервіс онлайн-знайомств Zoosk (30 мільйонів записів);
- Сервіс друку Снатbooks (15 мільйонів записів);
- Південнокорейська платформа моди SocialShare (6 мільйонів записів);
- Сервіс доставки їжі Home Chef (8 мільйонів записів);
- Торговий майданчик MINTED (5 мільйонів записів);
- Онлайн-газета CHRONICLE OF HIGHER EDUCATION (3 мільйони записів);
- Південнокорейський журнал про меблі GGuMim (2 мільйони записів);
- Медичний журнал MINDFUL (2 мільйони записів);
- Індонезійський інтернет-магазин BHINNEKA (1,2 мільйона записів);
- Американське видання STARTRIBUNE (1 мільйон записів).



Доступ до особистої інформації
73 мільйонів осіб



Обмежте введення свого номера телефону, що прив'язаний до онлайн-банкінгу, в будь-які онлайн-форми.

6. WANNAcry 2017



500,000 комп'ютерів



150 країн світу



\$1 млрд шкоди

Шкідлива **ПРОГРАМА-ВИМАГАЧ**, яка використовувала вразливість нульового дня в різних версіях Windows. Проникаючи в комп'ютери, вірус зашифрував весь вміст, а потім починав вимагати гроші за розблокування. Однак розшифрувати файли було неможливо. Вірус встиг заразити **500,000 комп'ютерів** в **150 країнах світу** і завдати шкоди в **\$1 млрд**. Найбільше постраждали **Росія, Україна** й **Індія**.

Регулярно оновлюйте програмне забезпечення.

7. КІБЕРАТАКИ МОЖУТЬ ВБИВАТИ?

На жаль, так. У 2015 році хакери зламали **САЙТ ASHLEY MADISON**, призначений для знайомств заміжніх жінок і одружених чоловіків. У результаті атаки витекли дані **40 млн користувачів**.

Частини з них почали розсилати загрози з вимогою **викупу в \$1,000**. Деякі з постраждалих злякалися, що їхні чоловік/дружина дізнається про зраду, і наклали на себе руки.



Витік даних
40 млн користувачів

Розсилання загроз з вимогою викупу в \$1,000



Залишайте якомога менше персональних даних в інтернет-банкінгу, в будь-які онлайн-форми.